PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-213553
(43)Date of publication of application : 06.08.1999

(51)Int.Cl. G11B 20/10
G09C 1/00
H04L 9/32

(21)Application number : 10-015788
(22)Date of filing : 28.01.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : KAMIBAYASHI TATSU
AKIYAMA KOICHIRO
TSUJIMOTO SHUICHI

(54) CONTRACT MANAGING DEVICE AND REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To make literary works audio-visual within the period of a contract by controlling the reproducing operation of a reproducing device with a signal transmitted to control the receiving operation of broadcasting waves based on an audio-visual contract.
SOLUTION: When a DVD-ROM is inserted into a DVD reproducing device and a reproduction is instructed, the device retrieves license information whose ID is matched with ciphered content information from a license storage part. When the license information corresponding to the ID of the content information exist, the efficiency of the license information is checked, and when the license information are not effective because the effective period of the information is expired or the like, the DVD reproducing device does not perform the decoding and the reproducing of the content information. On the other hand, when the information are effective, the device performs the decoding and the reproducing of the content information. Thus, a charge (a charge being an amount equivalent to a literary property) with respect to the viewing of the content information of a customer is replaced with the reception contract fee of a satellite broadcast in this manner.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－213553

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－15788

(22)出願日　平成10年(1998)１月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　辻本　修一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

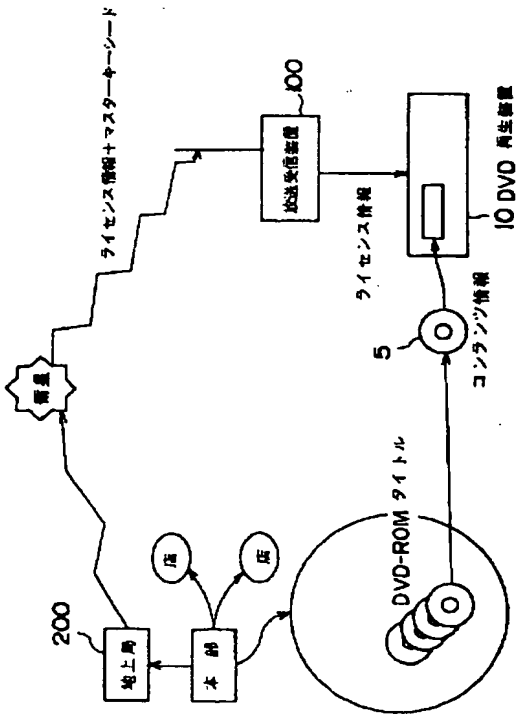
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　契約管理装置および再生装置

(57)【要約】

【課題】ディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル化された著作物の視聴の契約に基づく著作権の保護を前提としたディジタル情報の利用環境を提供する情報流通システムを提供する。

【解決手段】記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることを特徴とする。



【特許請求の範囲】
【請求項１】　記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、
個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、
視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することを特徴とする契約管理装置。
【請求項２】　記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、
個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、
前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることを特徴とする契約管理装置。
【請求項３】　前記鍵生成情報は、所定期間毎に更新されることを特徴とする請求項１または２記載の契約管理装置。
【請求項４】　放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、
前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、
この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、
を具備し、
前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることを特徴とする契約管理装置。
【請求項５】　放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、
前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、
この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、
を具備し、
前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することを特徴とする契約管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばＤＶＤ等の記録媒体にて暗号化されたコンテンツ情報を顧客に（有料）配布し、例えば衛星放送にてコンテンツ情報の復号鍵情報を含む制御情報を再生装置に配信して、そのコンテンツ情報の視聴契約（例えば、視聴期間）に応じて視聴可能にする情報流通システムに関する。
【０００２】
【従来の技術】近年、ディジタル情報処理技術や広帯域ＩＳＤＮ等の通信技術の発達、ＤＶＤ等の大容量、高画質、高音質を実現する高度な情報記録媒体の開発が進んでいる。このような情報の伝達手段の多様化、高度化が進むにつれ、ディジタル化された著作物等がネットワーク、記録媒体などを介して利用者の手元に大量に頒布され、利用者がそれらを自由に利用できる環境が生まれつつある。このような環境は、著作物の無断複製、無断改変、著作者の意図しない流通などが起こる機会を増大させるものであり、著作物の権利者にとって、自己の利益が不当に害されるのではないかという懸念を抱かせるものである。
【０００３】このような著作物の権利者の懸念を拭い払えるよう、迅速かつ手軽にディジタル化された著作物を流通させるとともに、適正にそれらを利用できるようなディジタル情報の利用環境を提供できる著作権の保護を前提としたシステムの開発は今後の重要な課題となる。
【０００４】ＤＶＤは、ＣＤ－ＲＯＭに代わる大容量のパソコンメディアであるとともに、映画、音楽、ゲーム、カラオケ等、様々な用途への広がりを期待でき、このようなＤＶＤの普及を図るために、ＤＶＤのタイトル価格を低く抑えたり、レンタルＤＶＤ市場への拡大も予想される。従って、このような観点からも、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物の所有ではなく利用に対して課金するという考えに基づく、情報に対する著作権の保護を前提とした情報の流通システムが不可欠となる。
【０００５】一方、ディジタル放送は、通信衛星（ＣＳ）に始まって、ケーブルＴＶ、地上放送へとディジタル化が進むにつれ、いっそうのサービスの充実が期待されており、これからの放送サービスの主役をつとめてい

くものと思われる。

【０００６】ディジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用でるため、高品質で均質なサービスの提供が可能となる。

【０００７】放送のディジタル化により、多様な情報形態（映像、音声、文字、データ等）によるマルチメディアサービスの提供が可能となり、そのようなサービスを提供するためのシステムも続々登場してきている。

【０００８】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャネルの番組の視聴を可能とするというものである。

【０００９】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャネル、契約期間に即して）しかも確実に提供する必要がある。

【００１０】

【発明が解決しようとする課題】そこで、本発明は、ディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル化された著作物の視聴の契約に基づく著作権の保護を前提としたディジタル情報の利用環境を提供する情報流通システムを提供することを目的とする。

【００１１】本発明は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる契約管理装置を提供することを目的とする。

【００１２】また、本発明は、放送配信される制御情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる再生装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することにより、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。

【００１４】また、本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることにより、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。

【００１５】本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることにより、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる。

【００１６】また、本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基

づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することにより、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる。

【００１７】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

（１）情報流通サービスの概要

図１は、本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示したものである。ディジタル化された著作物（例えば映画等）としてのコンテンツ情報は暗号化されて例えばＤＶＤ－ＲＯＭ等の記録媒体（以下、ＤＶＤ－ＲＯＭの場合を例にとり説明する）５に記録されて、例えばレンタル事業会社を介して配布される。

【００１８】レンタル事業会社の本部は、系列各店舗に例えば１タイトル毎の暗号化されたコンテンツ情報の記録されたＤＶＤ－ＲＯＭを配布する。顧客は所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入しただけでは該コンテンツ情報を視聴することはできない。ＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号、再生するための鍵情報（以下、コンテンツキー）が必要である。このコンテンツキーは、暗号化されて、例えばレンタル会社の本部と提携している衛星放送局２００から衛星放送にて各顧客が有する受信装置１００に配信される。

【００１９】顧客は系列店舗にて該コンテンツ情報のＤＶＤ－ＲＯＭを購入した際に、少なくとも視聴期間を定めた視聴契約に応じた料金を支払う。この視聴契約に基づき顧客が有するＤＶＤ－ＲＯＭの再生装置１０にて当該ＤＶＤ－ＲＯＭに記録されたコンテンツ情報を顧客が視聴できるようにすることが本発明の目的とするところである。

【００２０】なお、ＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号するコンテンツキーは、具体的には（以下の説明では）、衛星放送にて配信される一部暗号化されたライセンス情報（後述）に含まれている。

【００２１】ライセンス情報は、本実施形態の場合、例えば、レンタル会社の本部に設置されている契約管理装置にて生成される。顧客が有する再生装置１０には、受信装置１００（既存のものであることが望ましい）にて受信された衛星放送にて配信されるライセンス情報が入力し、例えば、別途衛星放送にて配信されるマスターキーシードに基づき生成されたマスタキーにて該ライセンス情報の暗号化部分を復号し、所定の判定処理（詳細は後述する）を実行して、当該顧客の行った視聴契約の有効範囲内での該コンテンツ情報の視聴が可能であると判断したときは、当該ライセンス情報に含まれるコンテンツキーを用いてＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号し、再生するようになっている。逆に、再生装置１０に有効なライセンス情報を入力しなければＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号することはできない。

【００２２】衛星放送にて配信されたライセンス情報は、各放送受信装置１００にて受信される。すなわち、本発明の情報流通サービスを利用しようとする顧客は、例えば、従来からある衛星放送の受信サービスを受ける場合と同様、予め当該衛星放送の受信契約を結んでいなければならない。さもなくば、放送受信装置１００にてライセンス情報を正しく取得することができない。

【００２３】放送受信装置１００にて受信されたライセンス情報は、再生装置１０へ送られるようになっている。再生装置１０は、入力されたライセンス情報を、再生装置機内部のライセンス情報蓄積部に保存する。

【００２４】ライセンス情報は、適当なスケジュールに従って、繰り返して放送されている場合がある。このスケジュール方式については後述する。ライセンス情報には、当該ライセンス情報の有効期限情報を含んでいてもよい。

【００２５】次に、本発明に係る情報流通サービスの概要を説明する。本発明に係る情報流通サービスを利用しようとする顧客は、このサービスに適応するＤＶＤ再生装置１０を購入し、さらに、該情報流通サービスを提供している事業会社の系列店舗から所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを取得するものとする。

【００２６】ＤＶＤ－ＲＯＭには、例えば、図２に示すように、暗号化されたコンテンツ情報が記録されている。所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入しても、該コンテンツ情報が暗号化されているため、そのままでは視聴することはできない。従って、このコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入する際には、必ずしも著作権相当量の料金を支払う必要が無い。すなわち、本発明に係る情報流通サービスを利用しようとする顧客は、例えば、「ＤＶＤ－ＲＯＭそのものの価格＋手数料」程度のきわめて低価格でＤＶＤ－ＲＯＭを取得することが可能となる。

【００２７】顧客は、購入した当該ＤＶＤ－ＲＯＭをＤＶＤ再生装置１０に挿入し、再生を指示すると、ＤＶＤ再生装置１０のライセンス情報蓄積部から、当該コンテンツ情報にＩＤに一致するライセンス情報を検索する。

初期のライセンス情報が存在しなければ、当該ＤＶＤ－ＲＯＭからコンテンツ情報の再生は行われない。当該コンテンツＩＤに対応するライセンス情報が存在する場合、ＤＶＤ再生装置１０は、ライセンス情報の有効性をチェックする。有効期限が経過しているなど、ライセンス情報が有効でない場合、ＤＶＤ再生装置１０は当該コンテンツ情報の復号再生を行わない。一方、ライセンス情報が有効であれば、ＤＶＤ再生装置１０は、当該コンテンツ情報の復号、再生を行う。

【００２８】このように、顧客のコンテンツ情報の視聴に対する課金（すなわち、著作権相当量の料金）は、衛星放送の受信契約料によって置き換えられる。情報流通サービスを利用しようとする顧客は、先ず、放送受信契約を結び、例えば、月々一定金額の受信料を支払う。次に、受信契約者はレンタル事業会社の系列店舗で、お好みのタイトルのコンテンツ情報を選ぶ。既に述べたように、暗号化コンテンツが記録された記録媒体の取得には、「記録媒体そのものの価格＋手数料」程度の金額を支払えばよい。その後、顧客は持ち帰ったコンテンツ情報をＤＶＤ再生装置１０で受信契約に応じて自由に再生することができる。放送受信装置１００からＤＶＤ再生装置１０に、最新の有効なライセンス情報が供給されているからである。

【００２９】例えば、ライセンス情報の放送配信によって、７月７日２３時５９分迄に配信されるライセンス情報（例えばコンテンツＩＤ「＃２１２４３」のコンテンツ情に対応するもの）は７月１４日２３時５９分と言う有効期限を持つとする。コンテンツＩＤ「＃２１２４３」のコンテンツ情報に対応するライセンス情報で、７月２１日２３時５９分と言う有効期限を有するものは、７月８日０時００分以降７月１４日２３時５９分迄に放送され、ＤＶＤ再生装置１０に格納される。これにより、顧客はコンテンツＩＤ「＃２１２４３」のコンテンツ情報を何時でも再生することができる。

【００３０】さて、当該放送の受信契約者が７月２２日付けで受信契約を解除する場合、契約解除の旨を７月１４日までにレンタル事業会社に通知する。然らば、当該顧客の受信装置１００は７月１４日２３時５９分を以ってライセンス放送の受信を中止する。この場合、７月１５日０時００分以降に放送される、有効期限７月２８日２３時５９を有するＩＤ「＃２１２４３」のライセンス情報は当該受信装置１００に配信されず、当該顧客のＤＶＤ再生装置１０に蓄積されることはない。

【００３１】従って、当該顧客は７月２１日２３時５９分以降は、ＩＤ「＃２１２４３」のコンテンツ情報を視聴できなくなる。以下、より具体的に本発明に係る情報流通サービスを提供するシステムについて説明する。

【００３２】ＤＶＤ－ＲＯＭには、図２に示すように、コンテンツキーにて暗号化されたコンテンツ情報と、該コンテンツ情報の識別情報（コンテンツＩＤ）と、該コンテンツ情報の内容を紹介するプロモーション用の情報とが記録されている。コンテンツＩＤとプロモーション用の情報とは暗号化されていない。なお、コンテンツキーは、各コンテンツ情報毎に異なる。また、コンテンツＩＤは、例えば、タイトル毎に１つづつ付与されているものとする。さらに、コンテンツキーはタイトル毎に予め定められたものである。

【００３３】図３は、ライセンス情報のデータ形式を具体例を示したもので、（ａ）図は、ライセンス情報に受信契約のなされた顧客の有する再生装置のそれぞれを識別するための識別情報（端末ＩＤ）を含まない場合のライセンス情報であり、（ｂ）図は当該ライセンス情報を受けとる再生装置を限定するための端末ＩＤを含む場合のライセンス情報を示している。

【００３４】図３（ａ）に示すライセンス情報は、コンテンツ情報の各タイトル毎に１つづつ生成されるもので、少なくとも当該タイトルのコンテンツＩＤ、コンテンツキーが含まれている。コンテンツＩＤは暗号化されず、それ以外の情報（少なくともコンテンツキー）はマスターキーにて暗号化されている。

【００３５】図３（ａ）に示したようなライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置１００に対し放送波受信可否を制御するための信号（ＯＮ／ＯＦＦ信号）を送ることにより行ってもよい。すなわち、例えば、顧客の視聴期間の開始時に当該顧客の放送受信装置１００に対しＯＮ信号を放送配信し、視聴期間の終了時に当該顧客の放送受信装置１００に対しＯＦＦ信号を放送配信する。放送受信装置１００が当該放送受信装置に対して配信されたＯＮ信号を受信することで放送波の受信を開始し、ＯＦＦ信号を受信することで放送波の受信を不可とする制御を行うようになっている。

【００３６】図３（ｂ）に示すライセンス情報は、少なくとも当該タイトルのコンテンツＩＤ、コンテンツキーと、当該ライセンス情報を受けとる再生装置を特定する端末ＩＤが含まれている。コンテンツＩＤは暗号化されず、それ以外の情報（少なくともコンテンツキー、端末ＩＤ）はマスターキーにて暗号化されている。

【００３７】なお、図３（ｂ）に示すライセンス情報は、端末ＩＤとして、単に個々の再生装置の端末ＩＤを１つのみ記載して、各顧客毎に当該ライセンス情報を生成、配信してもよいし、例えば端末ＩＤの下数桁を端末ＩＤとして記載して、１度に複数の再生装置が受け取れるようにしてもよい。後者の方がライセンス情報の配信効率がよいことは言うまでもない。

【００３８】図３（ｂ）に示すライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、ライセンス情報の端末ＩＤに契約期間がきれた顧客の再生装置１０の端末ＩＤを記載しないことで行うことができる。この

場合、再生装置１０のそれぞれがライセンス情報に含まれる端末ＩＤと自身の端末ＩＤとを比較してライセンス情報を取り込むか否かをチェックすることになる。契約期間中は自身の端末ＩＤそのものが記載された、あるいは自身の端末ＩＤを含むライセンス情報が頻繁に配信されるが、契約期間がきれた時点からライセンス情報には自身の端末ＩＤは記載されなくなる。従って、再生装置１０は、有効なライセンス情報を得られないがためにＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報の復号、再生が行えないことになる。

【００３９】ライセンス情報の暗号化には、次の様な特徴を持った暗号化方式を利用することが望ましい。

１）コンテンツＩＤ、コンテンツキーなどのデータを適当な順序で並べる。ここで、各データをフィールドと呼ぶことがある。

【００４０】２）　適当なアルゴリズムに従って、１）のビット列の順序を攪乱する。この際、広い範囲でビット攪乱が行われることが望ましい。

３）　２）のデータを適当な鍵と暗号方式で暗号化する。１）をそのまま暗号化しないのは、次の理由による。すなわち、通常の暗号方式は、あらかじめ定められた適当なビット長毎に暗号化を行うことを繰り返す。従って、２）の攪乱を行うことにより、ライセンス情報の各フィールドが分離・改変される危険性を低下させることが可能である。

【００４１】（２）契約管理装置

図４は、本実施形態に係る契約管理装置の構成例を示したもので、図１の地上局２００に設置されて用いられる。

【００４２】地上局２００は、図３（ａ）あるいは図３（ｂ）に示したようなライセンス情報とマスターキーシードを放送配信する。ライセンス情報中、コンテンツＩＤ以外の部分はマスターキーにて暗号化されている。ライセンス情報の機密性の向上のためにマスターキーは一定期間毎に更新することが好ましい。そのために、再生装置１０にてマスターキーを生成するために必要な情報、すなわち、マスターキーシードを（定期的あるいはマスターキー更新時に）放送配信するようになっている。

【００４３】さて、図４の契約管理装置は、ライセンス情報の生成、暗号化を行って放送配信するためのものである。顧客との間で放送受信契約がなされると、その契約内容（コンテンツＩＤ、視聴期間等）が、契約ユーザデータベース（ＤＢ）１に登録される。

【００４４】契約ユーザＤＢ１には、図５に示す形式でデータが蓄えられる。図５おいて受端末ＩＤは顧客の有する再生装置１０の端末ＩＤであり、この端末ＩＤに対応させて視聴契約のなされたコンテンツＩＤと視聴期間とが予め定められた形式で記憶されている。

【００４５】シードデータベース（ＤＢ）３は、マスターキー生成用のマスターキーシードから生成されるマスターキーをそのシードＩＤ及び有効期限とともに、図６に示す形式で格納している。シードＤＢ３にはシードＩＤに対応するマスターキーシードも格納されていてもよい。

【００４６】コンテンツキーデータベース（ＤＢ）４は、タイトル毎のコンテンツキーをコンテンツＩＤに対応させて図７に示す形式で格納している。次に、図３（ｂ）に示したようなライセンス情報を生成し、これを放送装置１３を使って受信装置に送る手順を図８に示すフローチャートを参照して説明する。

【００４７】ライセンス情報生成制御部９は、ライセンス情報生成部８に対し、ライセンス情報生成の指示を送る（ステップＳ１１）。この指示とは、例えば「１９９７年１２月１日から１ヶ月間契約している契約ユーザのライセンス情報を送れ」なる内容のもので、予め定められた形式のビット列で表現されたものでもよい。このような指示が出されるとライセンス情報生成部８では契約ユーザＤＢ１から１９９７年１２月１日から少なくとも１ヶ月間契約しているユーザ情報（図５参照）を検索して、当該情報を読み込む（ステップＳ１２～ステップＳ１３）。

【００４８】ここで、契約期間の最小単位は１ヶ月で、契約有効期限は１日にはじまり月末に終了するとし、マスターキーもこの契約最小期間に固有なものとする。すなわち、１１月のマスターキーは１２月のそれとは異なるものを用い、それぞれの月内では変更しないものとする。

【００４９】次に、付加情報生成部８は、コンテンツキーＤＢ４からコンテンツＩＤ毎のコンテンツキーを検索し（ステップＳ１５）、また、シードＤＢ３から１９９７年１２月１日から１９９７年１２月３１日に有効なシードに対応したマスターキーを検索する（ステップＳ１６）。

【００５０】以上によって得られた情報（コンテンツＩＤ、該コンテンツＩＤに対応するコンテンツキー、各ユーザの契約内容）をもとに、付加情報生成部８では、図３（ｂ）に示すようなライセンス情報を生成し、コンテンツＩＤ以外の情報を暗号化する（ステップＳ１７）。ここで生成されたライセンス情報は順次付加情報生成制御部９、放送装置１３に送られる。

【００５１】放送装置１３は、ライセンス情報を所定の周波数帯域の放送波に変換して受信装置に向けて放送配信する（ステップＳ１８）。スケジューリング部１４は、ライセンス情報ＤＢ５に格納されたライセンス情報を配信する際、あるいは、マスターキーシードを配信する際、各ユーザ側の受信装置にて確実にライセンス情報、マスターキーシードが受信されるように配信制御を行うものである。

【００５２】すなわち、例えば、受信契約後、契約変更

時、契約解約時、および、人気のタイトルのコンテンツＩＤに対するライセンス情報を送信する際には、当該ライセンス情報を頻繁に送る必要があり、そのためのライセンス情報の配信スケジューリングに従って、ライセンス情報の配信制御を行うのが、スケジューリング部１４である。

【００５３】ライセンス情報生成部８にて生成されたライセンス情報には、配信日時を示すタイムスタンプが含まれていてもよい。タイムスタンプの示す日時は時計１５にて計時されたできる限り正確なものであり、また、再生装置１０からは各種判定処理に用いる基準となる時刻となり得るものである。なお、タイムスタンプはもちろん暗号化されていない。

【００５４】図３（ａ）に示すようなライセンス情報を用いる場合には、契約ユーザＤＢ１を検索する必要がない。すなわち、図８のステップＳ１１でライセンス情報生成の指示を受けたライセンス情報生成部８は、ステップＳ１５に進み、コンテンツキーＤＢ４からコンテンツＩＤ毎のコンテンツキーを検索し、また、シードＤＢ３から１９９７年１２月１日から１９９７年１２月３１日に有効なシードに対応したマスターキーを検索し（ステップＳ１６）、図３（ａ）に示すようなライセンス情報を生成し、コンテンツＩＤ以外の情報を暗号化する（ステップＳ１７）。

【００５５】なお、マスターキーシードは、ライセンス情報の暗号化に用いられたマスターキーに対応するものをライセンス情報の配信と同時にあるいは適宜配信されている。

【００５６】（３）再生装置

図９は、本実施形態に係る再生装置１０の構成例を示したもので、図１０は、再生装置１０のライセンス判定ユニット２０８の構成例を示したものである。

【００５７】以下、図１１、図１２に示すフローチャートを参照して再生装置１０およびライセンス判定ユニット２０８の各構成部およびこれらの動作について説明する。放送受信装置１００は、地上局２００からの放送波を受信し、放送配信されたライセンス情報とマスターキーシードが再生装置１０のフィルタ２０２に入力する（ステップＳ２１）。

【００５８】フィルタ２０２ではライセンス情報とマスターキーシードとを分別し、マスタキーシードであれば、それをライセンス判定ユニット２０８へ転送し、ライセンス情報であれば、それをライセンス情報蓄積部２０４へ転送する（ステップＳ２２～ステップＳ２５）。

【００５９】ライセンス判定ユニット２０８では、マスターキー生成部８０１にてマスターキーシードからマスターキーを生成して、マスターキー格納部８０２に格納する（ステップＳ２６）。マスターキーを生成する際には、予め契約管理装置との間で定められた同一のアルゴリズムを用いてマスターキーシードから共有鍵としてのマスターキーを生成するようにしてもよい。また、ライセンス判定ユニット２０８のマスターキー生成部８０１では、新たにマスターキーシードが入力される度にそれを用いてマスターキーを生成して、それをマスターキー格納部８０２に格納されている前回までのマスターキーに上書きして保持することにより、マスターキーが更新されてもその都度その更新された新たなマスターキーを得ることができる。

【００６０】ライセンス情報蓄積部２０４では、入力されたライセンス情報をコンテンツＩＤ別に保存する。すなわち、ライセンス情報が入力される度に、それに含まれるコンテンツＩＤをチェックし、既に同じコンテンツＩＤのライセンス情報が保存されている場合は、それに上書きしていく。ライセンス情報にタイムスタンプが含まれている場合は、それに示される日時をチェックして、所定期間経過したものは廃棄する、新たに入力されたライセンス情報で上書きしていく、等の制御が行える。

【００６１】さて、再生装置１０にＤＶＤディスクが挿入されると（ステップＳ３１）、ＤＶＤドライブ２０６は、まず、当該ディスクからコンテンツＩＤを読み出し、ライセンス情報選択部２０７へ転送する（ステップＳ３２）。ライセンス情報選択部２０７は、当該コンテンツＩＤを有するライセンス情報を、ライセンス情報蓄積部２０４から検索する（ステップＳ３３）。当該コンテンツＩＤを有するライセンス情報が存在するときは、それをライセンス判定ユニット２０８に転送する（ステップＳ３４～ステップＳ３５）。当該ライセンスＩＤを有するライセンス情報が見つからないとき、あるいは、あったとしてもタイムスタンプに示される時刻から無効なもの（期限きれ）と判断できるときは、その後の処理を中止する。

【００６２】ラインセンス判定ユニット２０８の復号部８０４では、マスターキー格納部８０２に格納されているマスターキーを用いてライセンス情報選択部２０７から転送されたライセンス情報を復号する（ステップＳ３６）。

【００６３】ここで、図３（ｂ）に示したようなライセンス情報の場合のライセンス判定ユニット２０８の判定部８０５における判定処理について説明する。この場合、判定部８０５では、復号されたライセンス情報に含まれていた端末ＩＤにＩＤ格納部８０３に予め格納されている自身の端末ＩＤが一致するか、あるいは含まれているかをチェックする。自身の端末ＩＤと一致あるいは自身の端末ＩＤが含まれていれば当該ライセンス情報は有効と判定し、復号されたライセンス情報に含まれていたコンテンツキーをデコーダ（例えば、ＭＰＥＧ２デコーダ）２０９へ転送する（ステップＳ３７～ステップＳ３８）。それ以外の場合は、当該ライセンス情報は無効と判定し、以後の処理は中止する。

【００６４】次に、図３（ａ）に示したようなライセンス情報の場合のライセンス判定ユニット２０８の判定部８０５における判定処理について説明する。この場合、判定部８０５では、特に判定処理はおこなわなくてもよく、そのまま、復号されたライセンス情報に含まれていたコンテンツキーをＭＰＥＧ２デコーダ２０９へ転送する（ステップＳ３７～ステップＳ３８）。この場合の顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置１００に対し放送波受信可否を制御するための信号（ＯＮ／ＯＦＦ信号）を送ることにより行っているため、放送受信装置１００が一旦ＯＦＦ信号を受けたときはそれ以後ＯＮ信号を再び受信するまで放送波の受信動作を行うことはないからである。

【００６５】ＤＶＤドライブ２０６では、ＤＶＤディスクから暗号化されたコンテンツ情報を読み取って、それをＭＰＥＧ２デコーダ２０９へ転送する（ステップＳ３９）。

【００６６】ＭＰＥＧ２デコーダ２０９はライセンス判定ユニット２０８から転送されてきたコンテンツ情報を用いて該暗号化されたコンテンツ情報を復号し、さらにＤ／Ａ変換して所定の表示装置へ出力する（ステップＳ４０からステップＳ４１）。

【００６７】なお、ライセンス情報にタイムスタンプが含まれている場合、ライセンス判定ユニット２０８に時計が具備されているとき、判定部８０５では、タイムスタンプにて示されている日時と、この時計にて計時されている日時とを比較して、当該ライセンス情報の有効／無効を判定してもよい。また、ライセンス情報に含まれるタイムスタンプに示され時刻情報を用いて、当該時計の時間設定を行うようにしてもよい。これらの詳細処理動作は、特願平９－１２２５１１号に記載されている。

【００６８】

【発明の効果】以上説明したように、本発明の契約管理装置によれば、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。

【００６９】また、本発明の再生装置によれば、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることができる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示した図。

【図２】コンテンツ情報の記録された例えばＤＶＤ－ＲＯＭ等の記録媒体の記録データの構成例を示した図。

【図３】ライセンス情報のデータ構成例を示した図。

【図４】契約管理装置の構成例を示した図。

【図５】契約ユーザＤＢに記憶されるユーザ情報のデータ構成例を示した図。

【図６】シードＤＢに記憶される情報のデータ構成例を示した図。

【図７】コンテンツキーＤＢに記憶される情報のデータ構成例を示した図。

【図８】図４の契約管理装置の動作を説明するためのフローチャート。

【図９】再生装置の構成例を示した図。

【図１０】図９のライセンス判定ユニットの構成例を示した図。

【図１１】図９の再生装置および図１０のライセンス判定ユニットの動作を説明するためのフローチャート。

【図１２】図９の再生装置および図１０のライセンス判定ユニットの動作を説明するためのフローチャート。

【符号の説明】

放送管理装置

１…契約ユーザデータベース

３…シードデータベース

４…コンテンツキーデータベース

５…ライセンス情報データベース

８…ライセンス情報生成部

９…ライセンス情報生成制御部

１２…ライセンス情報出力要請部

１３…放送装置

１４…スケジューリング部

再生装置

２０２…フィルタ

２０４…ライセンス情報蓄積部

２０６…ＤＶＤドライブ

２０７…ライセンス情報選択部

２０８…ライセンス判定ユニット

２０９…ＭＰＥＧデコーダ

８０１…マスターキー生成部

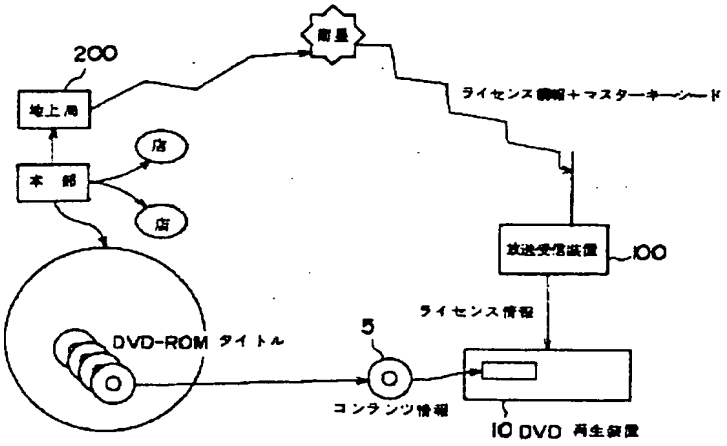
８０２…マスターキー格納部

８０３…ＩＤ格納部

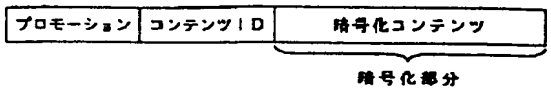
８０４…復号部

８０５…判定部

【図１】



【図２】

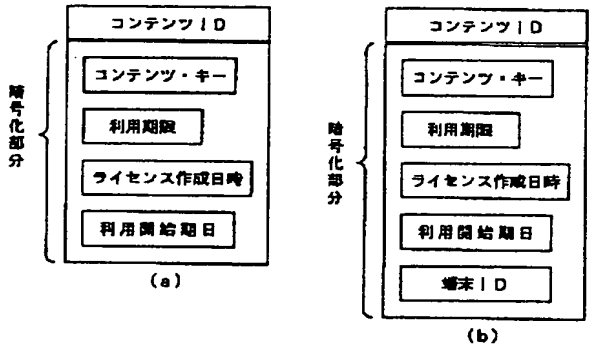


【図６】

シードＤＢ

シードＩＤ	マスターキー	有効期間

【図３】



【図５】

契約ユーザＤＢ

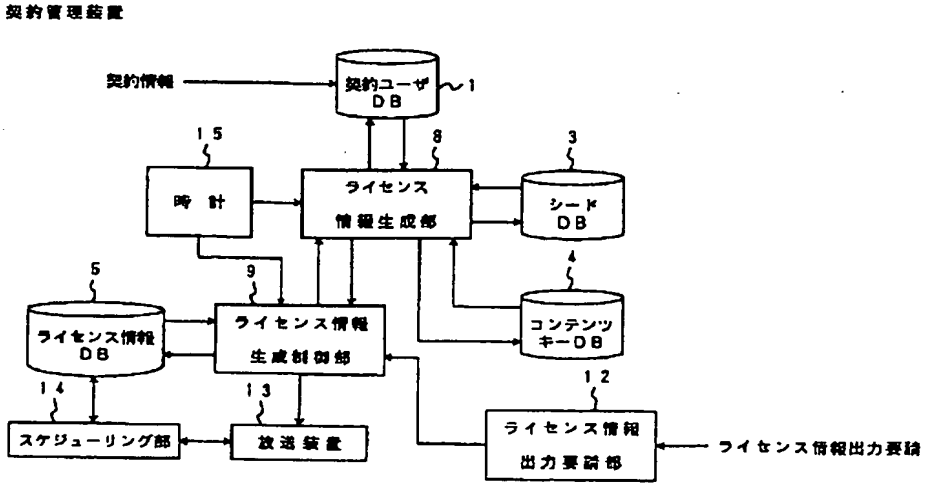
端末ＩＤ	コンテンツＩＤ	契約期間

【図７】

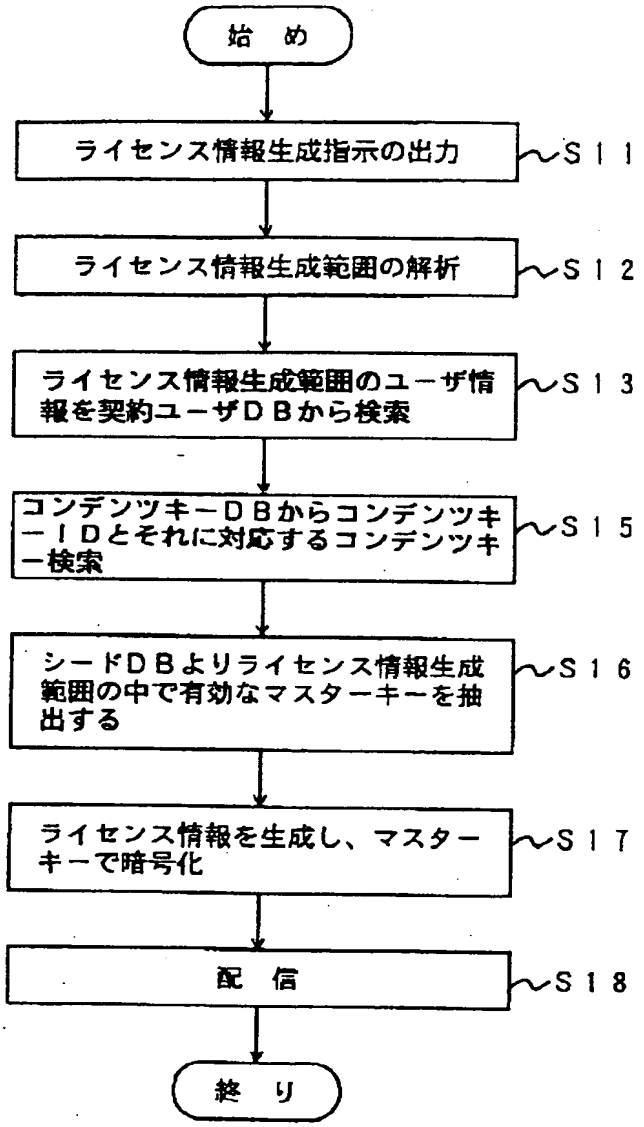
コンテンツキーＤＢ

コンテンツＩＤ	コンテンツキー

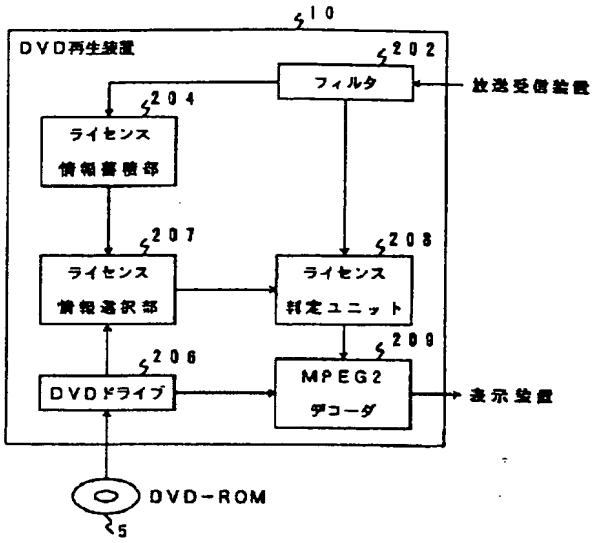
【図４】



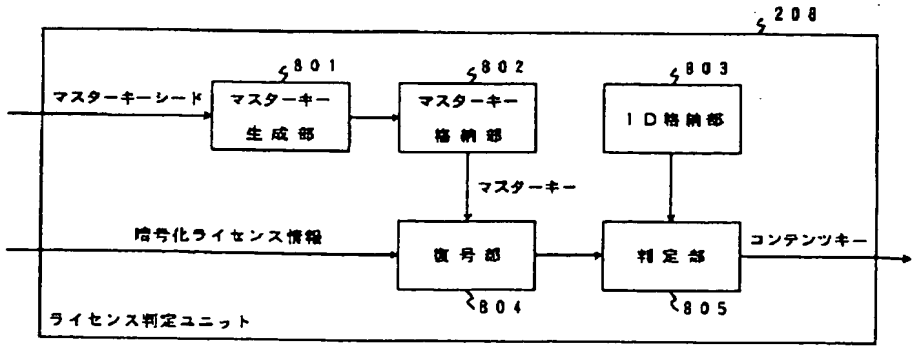
【図８】


始　め
ライセンス情報生成指示の出力
S１１
ライセンス情報生成範囲の解析
S１２
ライセンス情報生成範囲のユーザ情報を契約ユーザＤＢから検索
S１３
コンデンツキーＤＢからコンデンツキーＩＤとそれに対応するコンデンツキー検索
S１５
シードＤＢよりライセンス情報生成範囲の中で有効なマスターキーを抽出する
S１６
ライセンス情報を生成し、マスターキーで暗号化
S１７
配　信
S１８
終　り

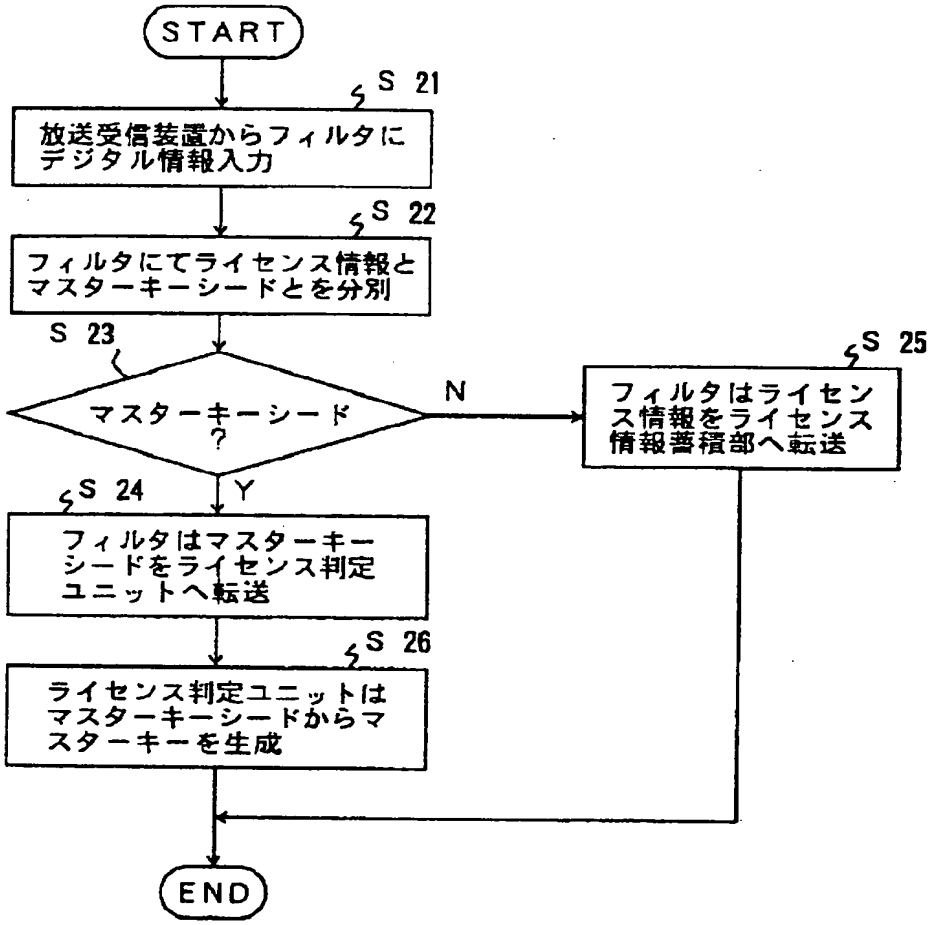
【図９】


１０
DVD再生装置
２０２
フィルタ
放送受信装置
２０４
ライセンス情報蓄積部
２０７
ライセンス情報選択部
２０８
ライセンス判定ユニット
２０６
DVDドライブ
２０９
MPEG2デコーダ
表示装置
DVD-ROM
５

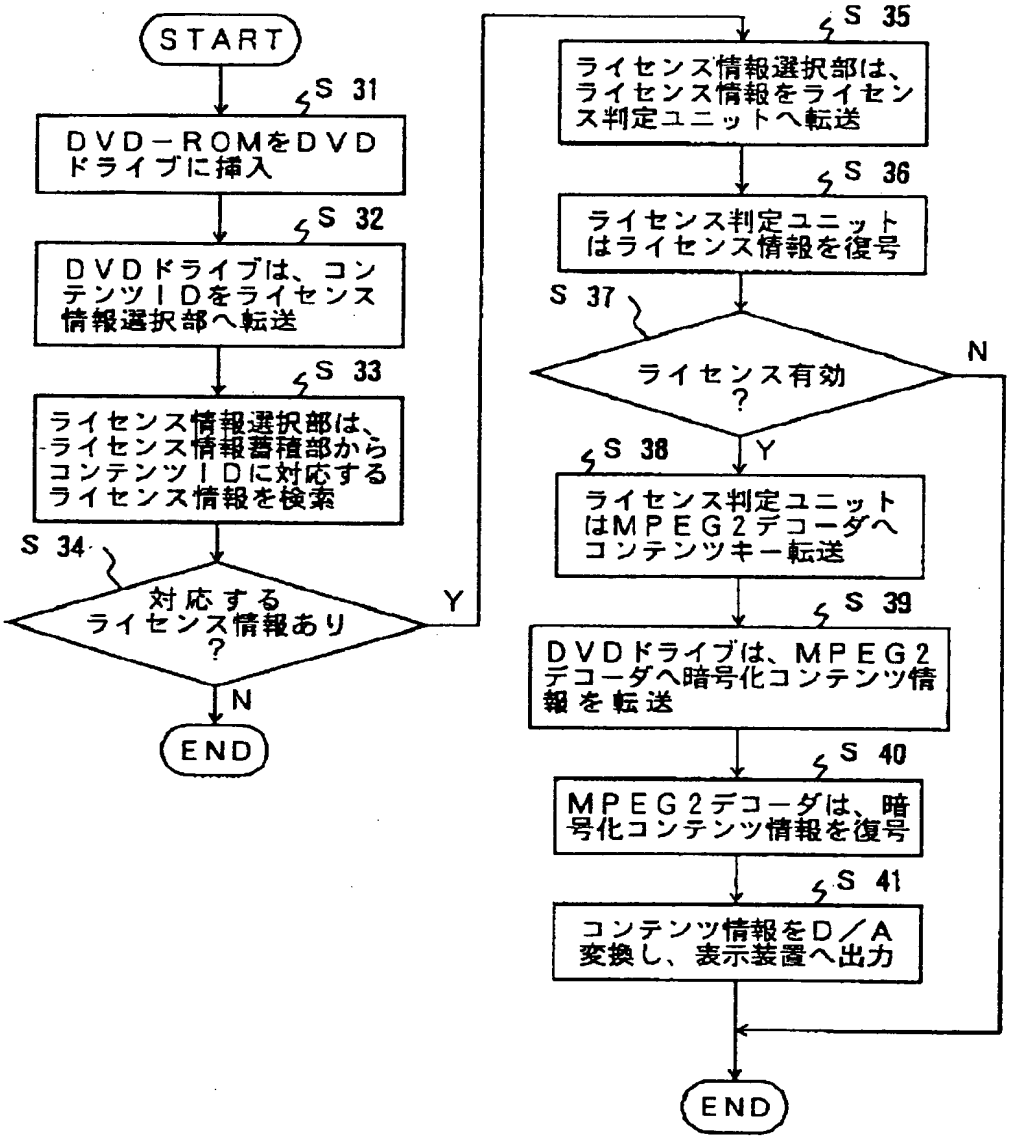
【図１０】


２０８
８０１
マスターキーシード
マスターキー生成部
８０２
マスターキー格納部
８０３
ＩＤ格納部
マスターキー
暗号化ライセンス情報
復号部
判定部
コンテンツキー
８０４
８０５
ライセンス判定ユニット

【図１１】


START
S 21
放送受信装置からフィルタにデジタル情報入力
S 22
フィルタにてライセンス情報とマスターキーシードとを分別
S 23
マスターキーシード？
N
S 25
フィルタはライセンス情報をライセンス情報蓄積部へ転送
Y
S 24
フィルタはマスターキーシードをライセンス判定ユニットへ転送
S 26
ライセンス判定ユニットはマスターキーシードからマスターキーを生成
END

【図１２】


START
S 31
DVD－ROMをDVDドライブに挿入
S 32
DVDドライブは、コンテンツＩＤをライセンス情報選択部へ転送
S 33
ライセンス情報選択部は、ライセンス情報蓄積部からコンテンツＩＤに対応するライセンス情報を検索
S 34
対応するライセンス情報あり？
Y
N
END
S 35
ライセンス情報選択部は、ライセンス情報をライセンス判定ユニットへ転送
S 36
ライセンス判定ユニットはライセンス情報を復号
S 37
ライセンス有効？
N
Y
S 38
ライセンス判定ユニットはＭＰＥＧ２デコーダへコンテンツキー転送
S 39
DVDドライブは、ＭＰＥＧ２デコーダへ暗号化コンテンツ情報を転送
S 40
ＭＰＥＧ２デコーダは、暗号化コンテンツ情報を復号
S 41
コンテンツ情報をＤ／Ａ変換し、表示装置へ出力
END